SECURITY SYSTEM

This invention relates to a security system and more particularly to a security management system for facilitating personnel identification and tracking within a secure area.

Conventional security management systems furnish a secure area with a network of transponder readers operable to interrogate transponders within their range and obtain from the transponders a unique identifier associated therewith. Users carry uniquely encoded transponders within the secure area.

Such security systems are inflexible and require a complex infrastructure in which security verification systems are incorporated within each transponder reader. One major drawback of such systems is that a stolen transponder can be used within the secure area and does not register as being stolen. Transponders are deemed valid until the unique transponder code is cancelled.

It is an object of the present invention to seek to provide a flexible security management solution requiring a minimum of system architecture.

Accordingly, one aspect of the present invention provides a security system for facilitating transponder carrier identification and tracking within a secure area comprising: an RF transponder having a memory in which is stored a unique identifier; and a transponder writer operable to send a replacement unique identifier to the transponder, the transponder replacing the identifier in the transponder memory with the replacement identifier.

Advantageously, the transponder has a fixed unit identifier serving to identify the transponder, the fixed unit identifier being a separate identifier to the unique identifier.

Preferably, the unique identifier comprises an identity code.

Conveniently, the unique identifier is encrypted and assigned by a security processor.

Advantageously, the transponder includes a transmitter to transmit the unique identifier.

Preferably, the transmitter is a contactless transmitter operable to transmit RF signals.

Conveniently, the transmitter is a contact transmitter operable to send signals to a unit in contact with the transponder.

Advantageously, the security system further comprises a transponder reader to receive from the transponder at least the unique identifier of the transponder.

Preferably, the transponder reader interrogates the transponder and, in response to the interrogation, receives from the transponder at least the unique identifier of the transponder.

Conveniently, the transponder reader is mounted within the secure area and has a location code which provides information as to the location of the transponder reader.

Advantageously, the transponder reader is portable and operable within the secure area.

Preferably, the transponder reader has a predetermined interrogation range such that a transponder within the interrogation range will receive an interrogation signal from the reader and will respond thereto by sending its unique identifier.

Conveniently, the security system further comprises a security processor having an access database setting out access parameters for the secure area and a carrier of a transponder, the security processor being operable to receive information from the transponder reader comprising at least the unique identifier of an interrogated transponder and the location of the transponder reader.

Advantageously, the security processor determines from consultation of the access database whether the carrier is authorised to be in the vicinity of the interrogating transponder reader and further determines what, if any, action needs to be taken.

Preferably, the security system further comprises an actuator controllable by the security processor to effect operation of a device in response to a condition determined by the security processor.

Conveniently, the device activated by the actuator is selected from the group consisting of: an image capture device; an alarm; an alert system; a lock; an emergency door release; a speaker; and a communication device.

Advantageously, the transponder is configured as a card having a contact terminal.

Preferably, a card reader/writer is provided having a contact region compatible with the card contact terminal, wherein the transponder is addressable by the card reader when the terminal and contact region are in contact with one another.

Conveniently, the card reader/writer is operable to write the replacement unique identifier to the transponder.

Advantageously, the card reader/writer is integrated with an identification authentication device so as to authenticate the identity of a carrier of the transponder prior to writing a replacement unique identifier to the transponder of the carrier.

Preferably, the carrier is selected from the group consisting of: personnel; a vehicle; and a hardware product.

Conveniently, the unique identifier has an expiry time after which the unique identifier is no longer valid.

Advantageously, the system is enabled by one of the following methods: Internet enabled, wireless enabled, hardwired, intranet enabled and combinations thereof.

Another aspect of the present invention provides a RF transponder for use in a security system for facilitating transponder carrier identification and tracking within a secure area comprising: a first memory in which is stored a replaceable

unique identifier; and a transmitter operable to send the unique identifier in response to an interrogation signal.

A further aspect of the present invention provides a RF transponder reader operable to send an interrogation signal to an RF transponder having a unique identifier and receive from the transponder, in response to the interrogation signal, the unique identifier, the reader being operable to transmit the unique identifier to a security processor for identity verification.

Preferably, the reader is a portable unit.

Conveniently, the reader is integrated with a data archiving system.

Advantageously, the data archiving system is a personal digital assistant.

Preferably, the reader incorporates a cellular telephone system.

Another aspect of the present invention provides a method of identity verification comprising the steps of: interrogating an RF transponder with an interrogation signal; receiving a unique identifier from the transponder provided in response to the interrogation signal; authenticating the identity of a user carrying the transponder; assigning a replacement unique identifier; and writing the replacement unique identifier to the transponder to replace the received unique identifier.

In order that the present invention may be more readily understood, embodiments thereof will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic representation of a security system embodying the present invention;

Figure 2 is a block diagram of the architecture of an exemplary security system embodying the present invention;

Figure 3 is a block diagram of a transponder embodying the present invention;

Figure 3A is a schematic plan view of the transponder of Figure 3;

Figure 4 is a block diagram of a transponder reader/writer, for use with the transponder of Figure 3;

Figure 5 is a block diagram of a portable transponder reader embodying the present invention for use with the transponder of Figure 3;

Figure 6A is a block diagram of a transponder reader embodying the present invention for use with the transponder of Figure 3;

Figure 6B is a block diagram of the transponder reader of Figure 6A provided with an immediate recognition unit;

Figure 7 is flow diagram of one possible mode of operation of the security system embodying the present invention;

Figure 8 is a flow diagram of a mode of operation of a security system embodying the present invention;

Figure 9 is a flow diagram illustrating a mode of operation of the security system embodying the present invention; and

Figure 10 is a flow diagram illustrating operation of a hand-held transponder for use with a security system embodying the present invention.

Referring to the drawings and, in particular, Figure 1, a security system embodying the present invention is described below in relation to a secure area 1 which is divided into a number of rooms or regions, to which authorised users 2 are allowed access. The nature of the access provided to users 2 is intended to be as flexible as possible, whilst at the same time, maintaining security to a required level.

A secure area 1 is provided with a plurality of transponder readers 3 each of which has a detection or interrogation range. It is intended that the number of blind spots, if any, is minimised in the secure area so the coverage provided by the transponder readers 3 is substantially blanket coverage. Further or additional coverage is provided by means of additional transponder readers 4 at access points such as doors, gates and/or barriers and hand-held units carried by security personnel as shown in Figure 1.

A central monitoring means comprises a security processor 5 which includes amongst other items an access database 6 which sets out for respective users of the system the access parameters attributable to each user and also sets out the access authority for respective regions, rooms, or areas within the secure area. The security processor 5 also maintains a log of user locations so as to facilitate user tracking within the secure area 1. Further, the security processor incorporates an encryption/decryption algorithm.

Typically, a "user" 2 refers to an individual person to whom a transponder 7 has been allocated. Transponders 7 are radio frequency (RF) transponders, 7 and are shown in more detail in Figure 3. Although the illustrated transponder 7 is an active transponder 7 having its own battery power, the use of passive transponders such as inductively coupled transponders is also envisaged. Active transponders are preferred because of their superior transmission range compared to passive transponders.

Referring to Figure 2, the block diagram shows an overall system architecture of the system components connected to a common bus 8. Although the components are shown in Figure 2 as being hard-wired, it is also possible for connection to the bus 8 to be effected by a wireless connection, intranet connection, Internet connection or the like.

The basic components of the security system are as follows:

RF transponders: As shown in Figure 3, each RF transponder 7 is configured as a card upon which a microcontroller is mounted for executing a transponder control program held in a ROM 10 and being connected to a memory 11 storing a renewable identification number referred to hereinafter as a unique identifier; and another memory or register 12 holding a fixed unit identifier number. Each transponder 7 is also provided with a transmitter 13 and receiver 14 connected to a built-in antenna 15. Further connectivity to the transponder 7 is provided by a contact region 16 on a surface of the card (see insert Figure 3a) to facilitate communication with the transponder 7 when in contact with a contact card reader. The transponders are operable upon receipt of an interrogation signal from a reader to transmit the unique identifier.

The unique identifier held in the memory 11 comprises an encrypted identity code assigned to the transponder by the security processor. The transponder itself does not include any encryption/decryption functionality serving to simplify the transponder design. All encryption/decryption functions are carried out by the security processor 5. The fixed unit identifier for each transponder 7 cannot be altered whereas the unique identifier held in the memory 11 of each transponder can be replaced/overwritten.

Transponder Readers: Transponder readers 3 are implemented in a number of ways and can be provided with further functionality. However, the most basic form of transponder reader is as shown in Figure 6A and comprises an antenna 17 for transmitting and receiving signals to/from the transponders 7 connected by an automatic switch 18 to respective transmitter 19 and receiver circuits 20 and then to a microprocessor 21 coupled to an oscillator 22 for transmitting received information from the transponders 7 to the security processor 5. Preferably, the uplink to the security processor 5 is at a different frequency or uses a different communication standard to the link with the transponder 7 - hence the need for the local frequency oscillator 22. The simplest form of transponder reader 3 acts simply as an interrogator and relay. The transponder readers 3 periodically send an interrogation signal to all the transponders 7 within the range of the signal transmitted by the transponder reader 3 and receive signals generated by the transponders 7 in response to receipt of the interrogation signal. The signal sent by the transponders 7 comprises a unique identifier which is relayed, in its encrypted form if encrypted, to the security processor 5.

The transponder readers 3 need not be wirelessly connected to the security processor but can also be hard-wired thereto over the bus 8.

As previously stated, such simple transponder readers 3 interrogate transponders 7 and relay identity codes of interrogated transponders to the security processor 5.

Transponder Reader/Writer: Transponder readers/writers 23 are slightly more complex than transponder readers 3 in that they also incorporate as their name would imply, a writing function, being able to communicate and send further information to the transponders 7. In addition to the functionality shown for the transponder reader of Figure 6A, the transponder readers/writers 23, such as that shown in Figure 4 are also able to send, in addition to an interrogation signal, a write signal to the transponders 7. The write signal is an encrypted unique identifier supplied to the reader/writer by the security processor 5. The encrypted unique identifier is written to the transponder memory 11 thereby overwriting the existing unique identifier in the memory 11.

As shown in Figure 4, the transponder reader/writer 23 can be further enhanced by the provision of one or more identification authentication devices 24 such as a keypad 25 for a password entry; a biometric authenticator 26 such as a finger print reader or retinal scan each of which is connected to the reader/writer's central processing unit 21 for communication by the communication bus 8 or wireless connection to the security processor 5.

In Figure 4, the communication between the transponder 7 and the reader/writer 23 is contactless. The reader/writer 23 can also be configured as a contact reader/writer such that the transponder 7 which is preferably configured as a card would be inserted into a slot provided in the reader/writer 23 to allow a contact region of the transponder card to be contacted by a terminal portion 16 of the reader/writer 23 so as to effect direct contact communication with the

card and read the transponder unique identifier and, if necessary, write a new replacement unique identifier to the transponder memory 11.

Additionally, as shown in Figure 4, an interactive display screen 27 may also be provided on the reader/writer.

The above-mentioned transponder readers 3 and transponder reader/writers 23 are physically mounted around the secure area 1 and at various access points 30. Each of the readers 3 and readers/writers 23 is provided with its own identifier so that when its information is transmitted to the security processor 5, the security processor can check on a look-up table or the like, the physical location of each reader 3 and reader/writer 23 as determined by its identifier.

Combining the physical location of the reader 3 and/or readers/writers 23 with the unique identifier of a detected transponder 7 gives the security processor 5 a log of transponder location over a period of time.

In order to offer further flexibility, the security system also provides portable transponder readers 31 and/or transponder readers/writers 32. An example of a portable transponder reader 31 is shown in Figure 5. In addition to the components required for a fixedly mounted transponder reader, the portable reader 31 is provided with a cellular transmission reception capability to enable communication with the security processor. The cellular transmissions/reception capability also allows the portable reader to be used as a cellular telephone to communication with other portable readers or third parties. Preferably, the portable reader is provided with a rechargeable battery power source and an interactive touch screen display.

The transponder reader of Figure 6A can be integrated with a motion detector such as a conventionally available infra red motion detector so that it is triggered to send an interrogation signal upon detection of movement within its detection zone so as to determine the identity of the user causing movement. Clearly, if the moving object does not have a transponder associated with it which is authorised to be in that area, then an appropriate signal indicating this is sent to the security processor.

The above discussion pre-supposes that a transponder is carried by each authorised user. However, transponders can also be carried by inanimate objects such as vehicles or portable devices such as expensive hardware.
The transponder must be carried by the user at all time and visibly seen by the security personnel on duty. Each transponder stores, for sending upon receipt of an interrogation signal at least the encrypted unique identifier associated with the authorised user. In some embodiments, the transponder can send a combination of the unique identifier and the fixed unit identifier.

A user carrying a transponder 7 with an authorised unique identifier is allowed to access certain areas and doors in accordance with predefined authorisation and/or access parameters held by the security processor 5.

The authorisation parameters shall include exact "start-work" and "stop-work" times of a user; a user authority level; a number of permissible entries of a user at a specific door or gantry; and a security procedure for gaining access to predetermined areas. An attempt to gain access outside these parameters will lead to an output from the security processor to effect actuators to activate one or more of the following: alarms, "silent" alarms (for security personnel) and shutting and/or locking of doors and access points.

At the end of a pre-defined working time, a transponder will automatically lose certain accesses to doors, gantries or areas. Accordingly, at the end of a day or at a pre-defined time, the unique identifier of a transponder will be completely disabled. Thus, an authorised user is not allowed to stay within certain restricted zones or compound safeguarded by the security management system after his/her duty.

To re-enter the secure area, the user has to undergo a "check-in" process.

During the "check-in" process at the security checkpoint (refer to Fig 1), the user's identity will be verified by the security personnel on duty. At the same time, the user is required to insert his/her transponder card into a contact transponder reader/writer for the assignment of a new unique identifier assigned by the security processor and associated with the access parameters stored at the security processor.

This new unique identifier allows the user to re-access the doors, gantries or area he/she is authorised to and allows the user to perform his/her daily duty.

Such an implementation of the security system drastically decreases the changes of intrusion with a stolen card, as well as blocking unauthorised staff from entering restricted zones. Validity durations or expiry times of unique identifiers can be tailored to restricted zones by the authorisation parameters held by the security processor but basically, the shorter the validity time of a unique identifier to a door, gantry or area, the more secure the restricted zone.

Also, the image of entire "check-in" process for each transponder is recorded by an image capture device 40 such as a CCD camera or the like, is transferred and stored by the security processor in an archive.

Next, in the compound safeguarded by the security management system, transponder readers are installed which have a predetermined detection or interrogation range. The role of the transponder readers is purely to receive the encrypted unique identifier and relay the same to the security processor for identity verification and to update a log of transponder location and movement. By not integrating a built-in security verification system in each transponder reader, like other conventional security systems, fabrication costs are reduced to a minimum. Ultimately, this makes for an affordable security management system yet provided with blanket coverage.

Besides, the compound is further patrolled by security personnel, who are each equipped with a portable transponder reader. Ideally, said portable transponder reader is integrated with an RF transponder reader/writer; cellular telephone system; and security data archiving. Preferably, the detection range is 5 metres or above.

Transponder readers are also provided at acces points such as doors, integrated into the security management system. This is used to verify the unique identifier of a transponder at a door or a gantry. The reader sends the received unique identifier to the security processor for verification against the authorisation parameters via a wireless communication system.

The security management system allows security personnel to monitor and track the positions of all transponders within the secure area with reference to the reader identifiers and the transponder unique identifiers.

The security processor is the central identity verification database, which provides related information and photographs of a transponder holder, a log of a transponder as well as the present location of a transponder. Also, it activates input/output actuators in response to the pre-defined authorisation parameters.

If an intruder is detected, instructions are transmitted to all portable transponder readers and the checkpoint(s). Also, information relating to the particular transponder and the holder thereof, such as last location detected by detecting mean, track records of the transponder, personal information of transponder holder and a snap-shot of transponder holder's image during the latest check-in, are enclosed to assist the patrolling security personnel in identifying the intruder.

Furthermore, the particular unique identifier is immediately disabled and input/output logics for shutting doors are activated.

Figure 2 depicts an overview of security management system architecture. Examples of the present invention provide a unique security management system for authenticating and tracking people as well as vehicles in public areas or high security zones. Public areas in the present context includes secure workplace environments, airports, banks, tourist spots, shopping mall, etc. Likewise, high security zones include military bases and hazardous material storage areas.

The system can be hardwired, Internet enabled, intranet enabled, wireless enabled or in any combination thereof.

Figures 7, 8, 9 and 10 outline related process flows of the security management system. Said process flows are adequate for the major components in the system to carry out their roles as shown in Figures 1 and 2 and described in relation thereto. Therefore, it should not be limited to the proposed process flows if additional components are integrated in the system.

In Figure 7, the process flow of detecting a transponder is shown. In the security management system, a detecting mean periodically transmits an interrogation signal. The interrogation signal is received by the transponders falling within range of the transponder reader. This prompts the transponder to transmit an encrypted unique identifier to the reader.

Next, the reader receives the unique identifier and via the Internet, intranet or wireless communication, the detected unique identifier is then transferred to the security processor where the unique identifier is de-coded. It is subsequently verified against the identity database with respect to pre-defined authorisation parameters.

If a negative result is obtained, input/output signals will immediately be sent to activate emergency input/output logics of field sensors and if necessary, display records and give specific instructions to portable transponder readers. The particular unique identifier will be disabled and all subsequent movements of the particular transponder will be recorded.

On the other hand, if a positive result is obtained, the tracking record or log of the particular unique identifier will be updated. Besides, an input/output signal will also be sent to update the monitoring means in the field.

In Figure 8, the process flow of an integrated motion detector and transponder reader is shown. The process flow is similar to Figure 7 except that the device is in standby mode until activated by the motion detector identifying a moving object.

In Figure 9, the process flow of writing a new replacement unique identifier to the transponder is shown. To implement a better security procedure to a restricted zone, a unique identifier should ideally expiry within a specified time. In this example, a transponder can be programmed such that, its unique identifier will expiry after one day (for example). The user is then required to renew or obtain a fresh identity number via a transponder reader and writer.

By inserting a transponder card (for a contact reader/writer) or coming into close proximity with (for a contactless reader/writer) a reader/ writer and subsequently performing some other means of identity verification procedure, such as biometric and password, the reader/writer will execute its verification procedures. If a negative result is obtained, the unique identifier will immediately be disabled and a security administrator will be activated. If a positive result is achieved, then this prompts the transfer of the read and encrypted unique identifier to the security management system via the Internet, intranet or wireless communication. Next, the unique identifier is decrypted and verified against the identity database with respect to pre-defined authorisation parameters.

If a negative result is obtained, input/output signals will immediately be sent to activate emergency input/output logics of field sensors, as well as give specific instruction to other handheld detectors. The particular unique identifier will be disabled and all subsequent movements of the particular transponder will be recorded.

On the other hand, if a positive result is obtained, a new unique identifier will be generated by the security processor 5 and the identity and access databases will be updated. Following that, said new unique identifier will be encrypted by the security processor 5, transferred to the reader/writer 23 and written into the transponder memory 11 in place of the previously stored unique identifier.

For position tracking purpose, the tracking record of the particular unique identifier will be updated. An input/output signal will also be sent to update the monitoring means in the field.

In Figure 10, the process flow for a portable transponder reader is shown. The process flow is similar to that of a simple transponder reader. However, said detecting mean is a portable security unit. It is specially designed for security personnel to perform random verification on the users within the restricted zone. This portable transponder reader has a built-in standard cellular telephone system for communications between handheld units and a central despatch station.

In the present specification "comprises" means "includes or consists of" and "comprising" means "including or consisting of".

The features disclosed in the foregoing description, or the following claims, or the accompanying drawings, expressed in their specific forms or in terms of a means for performing the disclosed function, or a method or process for attaining the disclosed result, as appropriate, may, separately, or in any combination of such features, be utilised for realising the invention in diverse forms thereof.